

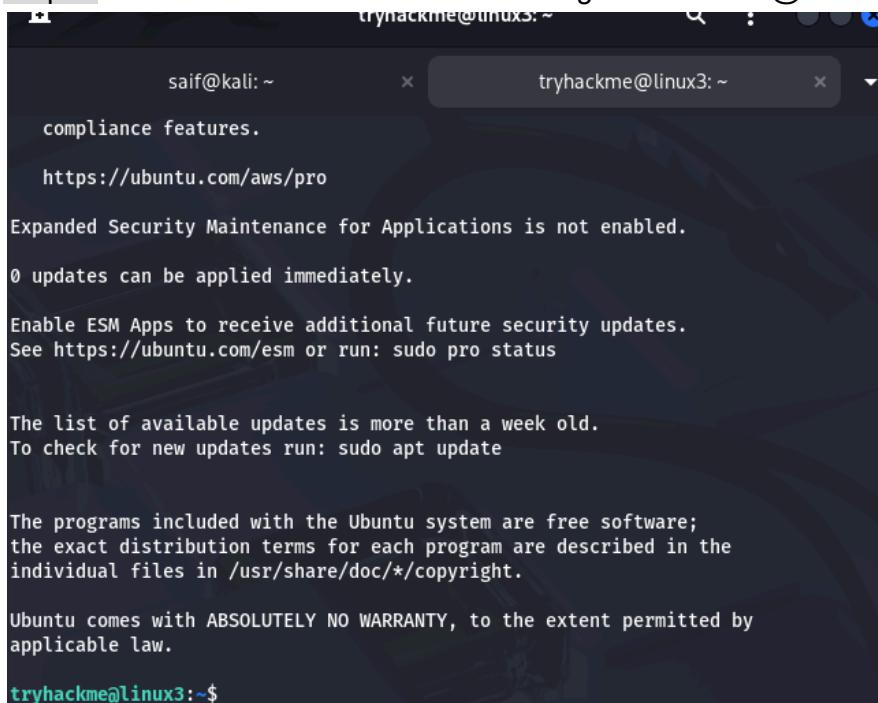
Room: Linux fundamentals part 3, task-8

Objective: getting IP address of a user from log file

Tool used: nano (for log file reading), ssh (for connecting to THM machine)

## Steps

Step-1: Connect to the remote machine using the “ssh user@userIP” command.



```
saif@kali: ~          tryhackme@linux3: ~
compliance features.

https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

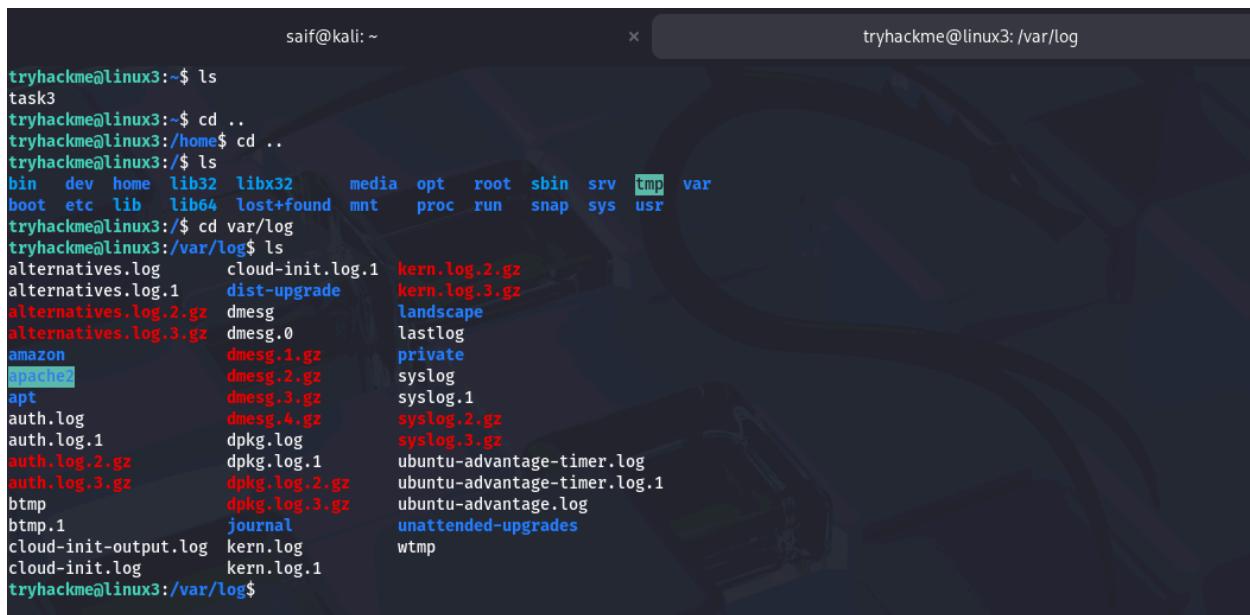
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

tryhackme@linux3:~$
```

Step-2: go to the logs folder using “cd” and “ls” commands.

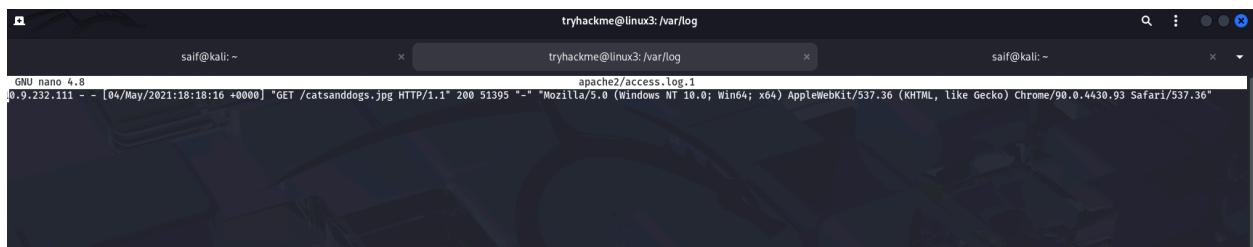


```
saif@kali: ~          tryhackme@linux3: /var/log
tryhackme@linux3:~$ ls
task3
tryhackme@linux3:~$ cd ..
tryhackme@linux3:/home$ cd ..
tryhackme@linux3:~/ls
bin dev home lib32 libx32 media opt root sbin srv tmp var
boot etc lib lib64 lost+found mnt proc run snap sys usr
tryhackme@linux3:$ cd var/log
tryhackme@linux3:/var/log$ ls
alternatives.log  cloud-init.log.1  kern.log.2.gz
alternatives.log.1  dist-upgrade   kern.log.3.gz
alternatives.log.2.gz  dmesg      landscape
alternatives.log.3.gz  dmesg.0    lastlog
amazon            dmesg.1.gz  private
apache2           dmesg.2.gz  syslog
apt               dmesg.3.gz  syslog.1
auth.log          dmesg.4.gz  syslog.2.gz
auth.log.1        dpkg.log   syslog.3.gz
auth.log.2.gz     dpkg.log.1  ubuntu-advantage-timer.log
auth.log.3.gz     dpkg.log.2.gz  ubuntu-advantage-timer.log.1
bttmp             dpkg.log.3.gz  ubuntu-advantage.log
bttmp.1          journal   unattended-upgrades
cloud-init-output.log  kern.log  wtmp
cloud-init.log    kern.log.1
tryhackme@linux3:/var/log$
```

Here we can see all types of .log files. Our goal is to find out the IP of a user who visited a site. So we can find that log inside the “apache2” folder.

```
tryhackme@linux3:/var/log$ ls -l apache2
total 12
-rw-r----- 1 root      adm        0 Feb  3  2025 access.log
-rwxrwxrwx  1 tryhackme tryhackme 209 May  4 2021 access.log.1
-rw-r----- 1 root      adm        0 Feb  3  2025 error.log
-rw-r----- 1 root      adm       810 Oct 18 2022 error.log.1
-rwxrwxrwx  1 root      adm       464 May  5 2021 error.log.2.gz
-rw-r----- 1 root      adm        0 May  4  2021 other_vhosts_access.log
tryhackme@linux3:/var/log$
```

**Step-3:** Inside the apache2 folder we have permission to read “access.log.1” and “error.log.2.gz”. In that case we will try to read both of these files to check if we get some info. We will use nano for that.



IP: 10.9.232.111

File tried to access: catsanddogs.jpg